

#3

Docket No. 826.1606/JDH

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:)
)
Haruyasu UEDA)
)
Serial No.: Not Assigned)
)
Filed: May 25, 2000)
)
For: DEVICE, METHOD AND STORAGE)
MEDIUM TO BLOCK JUNK EMAIL)

Group Art Unit: Not Assigned

Examiner: Not Assigned

JC531 U.S. PTO
09/577594
05/25/00

**SUBMISSION OF CERTIFIED COPY OF PRIOR FOREIGN
APPLICATION IN ACCORDANCE
WITH THE REQUIREMENTS OF 37 C.F.R. §1.55**

*Honorable Commissioner of
Patents and Trademarks
Washington, D.C. 20231*

Sir:

In accordance with the provisions of 37 C.F.R. §1.55, the applicant(s) submit(s)
herewith a certified copy of the following foreign application:

Japanese Patent Application No. 11-147680, filed: May 27, 1999.

It is respectfully requested that the applicants be given the benefit of the foreign filing
date as evidenced by the certified papers attached hereto, in accordance with the requirements
of 35 U.S.C. §119.

Respectfully submitted,
STAAS & HALSEY LLP

Date: May 25, 2000

By:

James D. Halsey, Jr.
Registration No. 22,729

700 Eleventh Street, N.W.
Suite 500
Washington, D.C. 20001
(202) 434-1500

PATENT OFFICE
JAPANESE GOVERNMENT

JC531 U.S. PTO

09/577594



This is to certify that the annexed is a true copy of the
following application as filed with this Office.

Date of Application: May 27, 1999

Application Number: Patent Application
No. 11-147680

Applicant(s): FUJITSU LIMITED

February 14, 2000

Commissioner,
Patent Office

Takahiko KONDO

Certificate No.2000-3006569

日 本 国 特 許 庁

PATENT OFFICE
JAPANESE GOVERNMENT

JC531 U.S. PTO
09/577594
05/25/00

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日

Date of Application:

1999年 5月27日

出 願 番 号

Application Number:

平成11年特許願第147680号

出 願 人

Applicant(s):

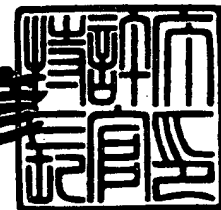
富士通株式会社

CERTIFIED COPY
PRIORITY DOCUMENT

2000年 2月14日

特許庁長官
Commissioner,
Patent Office

近 藤 隆 彦



出証番号 出証特2000-3006569

【書類名】 特許願

【整理番号】 9900731

【提出日】 平成11年 5月27日

【あて先】 特許庁長官殿

【国際特許分類】 H04L 9/00

【発明の名称】 悪戯メール防止装置、その方法及び記録媒体

【請求項の数】 18

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

【氏名】 上田 晴康

【特許出願人】

【識別番号】 000005223

【氏名又は名称】 富士通株式会社

【代理人】

【識別番号】 100074099

【住所又は居所】 東京都千代田区二番町8番地20 二番町ビル3F

【弁理士】

【氏名又は名称】 大菅 義之

【電話番号】 03-3238-0031

【選任した代理人】

【識別番号】 100067987

【住所又は居所】 神奈川県横浜市港北区太尾町1418-305 (大倉山二番館)

【弁理士】

【氏名又は名称】 久木元 彰

【電話番号】 045-545-9280

【手数料の表示】

【予納台帳番号】 012542

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9705047

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 悪戯メール防止装置、その方法及び記録媒体

【特許請求の範囲】

【請求項 1】 悪戯メールを防止する装置であって、

受信した電子メールからメールアドレスを抽出するメールアドレス抽出手段と

、
特定のメールアドレス、または、特定のメールアドレスパターンに対応して、
該受信した電子メールの処理方法を登録する記憶手段と、

該受信した電子メールのメールアドレスと該記憶手段に記憶されているメールアドレス、または、メールアドレスパターンとの照合を行い、該照合の結果得られた処理方法に基づいて、該受信した電子メールを処理するメール処理手段と、
を備えることを特徴とする装置。

【請求項 2】 特定の性質を持ったメールとそれ以外のメールを区別して処理
するよう指定する指定手段を更に備えることを特徴とする請求項 1 に記載の装置

。
【請求項 3】 暗号化された処理方法を解釈して処理する手段を更に備えるこ
とを特徴とする請求項 1 に記載の装置。

【請求項 4】 電子メールを受信する受信手段と、受信した全ての電子メール
を、送信元のアドレスを付加して配信する手段とを備える電子メールサーバから
電子メールを受信する装置であって、

受信した電子メール中に含まれている、送信元のアドレスを解釈して、特定の
メールアドレス、あるいは特定のメールアドレスパターンに対する処理方法を設
定する手段を備えることを特徴とする装置。

【請求項 5】 特定の性質を持ったメールとそれ以外のメールを区別して処理
するよう指定する指定手段を更に備えることを特徴とする請求項 8 に記載の装置

。
【請求項 6】 暗号化された処理方法を解釈して処理する手段を更に備えるこ
とを特徴とする請求項 4 に記載の装置。

【請求項 7】 電子メールを送信するときに自分のアドレスとして発行したア

ドレスを、付加的な情報と関連づけて記録しておき、該付加的な情報を必要に応じて表示することを特徴とする請求項 4 に記載の装置。

【請求項 8】前記電子メールの送信時に発行したアドレスと該電子メールの送信相手を記録しておき、その後、該送信相手にメールを送信する際には、自分のアドレスとして該発行したアドレスを使うことを特徴とする請求項 4 に記載の装置。

【請求項 9】悪戯メールを防止する方法であって、

(a) 受信した電子メールからメールアドレスを抽出するステップと、

(b) 特定のメールアドレス、または、特定のメールアドレスパターンに対応して、該受信した電子メールの処理方法を登録するステップと、

(c) 該受信した電子メールのメールアドレスと該ステップ (b) で記憶されたメールアドレス、または、メールアドレスパターンとの照合を行い、該照合の結果得られた処理方法に基づいて、該受信した電子メールを処理するステップと

を備えることを特徴とする方法。

【請求項 10】特定の性質を持ったメールとそれ以外のメールを区別して処理するよう指定するステップを更に備えることを特徴とする請求項 9 に記載の方法。

【請求項 11】暗号化された処理方法を解釈して処理するステップを更に備えることを特徴とする請求項 9 に記載の方法。

【請求項 12】電子メールを受信する受信手段と、受信した全ての電子メールを、送信元のアドレスを付加して配信する手段とを備える電子メールサーバから電子メールを受信する方法であって、

受信した電子メール中に含まれている、送信元のアドレスを解釈して、特定のメールアドレス、あるいは特定のメールアドレスパターンに対する処理方法を設定するステップを備えることを特徴とする方法。

【請求項 13】特定の性質を持ったメールとそれ以外のメールを区別して処理するよう指定するステップを更に備えることを特徴とする請求項 12 に記載の方法。

【請求項 1 4】暗号化された処理方法を解釈して処理するステップを更に備えることを特徴とする請求項 1 2 に記載の方法。

【請求項 1 5】電子メールを送信するときに自分のアドレスとして発行したアドレスを、付加的な情報と関連づけて記録しておき、該付加的な情報を必要に応じて表示することを特徴とする請求項 1 2 に記載の方法。

【請求項 1 6】前記電子メールの送信時に発行したアドレスと該電子メールの送信相手を記録しておき、その後、該送信相手にメールを送信する際には、自分のアドレスとして該発行したアドレスを使うことを特徴とする請求項 1 2 に記載の方法。

【請求項 1 7】コンピュータに、

(a) 受信した電子メールからメールアドレスを抽出するステップと、

(b) 特定のメールアドレス、または、特定のメールアドレスパターンに対応して、該受信した電子メールの処理方法を登録するステップと、

(c) 該受信した電子メールのメールアドレスと該ステップ (b) で記憶されたメールアドレス、または、メールアドレスパターンとの照合を行い、該照合の結果得られた処理方法に基づいて、該受信した電子メールを処理するステップと

、
を備える処理を実行させるコンピュータ読み取り可能なプログラムを記録している記録媒体。

【請求項 1 8】電子メールを受信する受信手段と、受信した全ての電子メールに、送信元のアドレスを付加する手段とを備える電子メールサーバから電子メールを受信するコンピュータに、

受信した電子メール中に含まれている、送信元のアドレスを解釈して、特定のメールアドレス、あるいは特定のメールアドレスパターンに対しての処理方法を設定するステップを備える処理を実行させるコンピュータ読み取り可能なプログラムを記録している記録媒体。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、電子メールに係り、特に、悪戯メールの防止方法及び防止装置に関する。

【0002】

【従来の技術】

今日、インターネットが一般に普及し、インターネットを介して多くの情報がやりとりされる様になった。情報のやりとりの中には、ホームページによる情報の公開の他に、従来からあった、電子メールでの情報のやりとりがある。ところが、今日では、個人の電子メールアドレスが、予期せぬ相手に漏洩し、不要な電子メールが大量に送られてくるという問題が発生している。従来、SPAMと呼ばれる宣伝や悪戯のためのメールの被害を防止するためには、電子メールソフトで対応する必要があった。このような、SPAM防止方法に於いては、SPAMにしばしば現れる文字列を検出したり、特定のメールアドレスから送られてくるものを除くことは可能だったが、そのような方法を提供する米国特許5619648号では、本質的な解決にはならず、SPAM送信の手口がどんどん複雑になって、いたちごっこになるだけであった。

【0003】

また、まれにだが、本来受け取りたいメールをSPAMと間違えて除いてしまったために読めなくなるという危険もあった。すなわち、同じ文字列を含む電子メールであっても、その文字列の示す内容を勧誘するものと、その文字列で表される内容に対する反対意見を述べるものとがあり、文字列の検出のみによって受信したメールの要／不要を決めるのは、おのずと限界がある。

【0004】

また、電子メールアドレスを教える機会がどんどん増えるにつれ、どこからSPAM相手にメールアドレスが知られてしまったのかを追跡することはほとんど不可能であった。すなわち、今日では、個人がホームページを開設し、情報を公衆に向けて発信するということが多くなったが、ホームページに掲載される情報に対する責任の所在を明らかにするために、ホームページへの情報の掲載者のメールアドレスを公開することが行われている。このような場合、メールアドレスが世界中のどのような人に見られているか分からず、悪戯メールが送られてくる

可能性も非常に高くなって来ている。

【0 0 0 5】

なお、電子メールの処理方法は、既に公知であるので、詳細な説明は以下の説明に於いて省略する。電子メールの処理方法の詳細については、例えば、「send mailシステム管理」Bryan Costales、Eric Allman著、株式会社オライリー・ジャパン発行、オーム社発売、あるいは、Network Information Center (NIC) から配布されるRFC (Request For Comments) を参照されたい。

【0 0 0 6】

【発明が解決しようとする課題】

従来のシステムにおいても、自分の電子メールアドレスが、SPAMの対象となってることが分かった時点で電子メールアドレスを変更することは不可能ではなかったが、従来のシステムは、電子メールのアドレスは一人につき一つずつ割り当てられており、料金もアドレス一つにつき一定額であることが多いため、SPAMによる被害を受けるたびにプロバイダとの契約の変更をしたり、通常使う電子メールアドレスを変更したり、人に教えた電子メールアドレスを変えてもらったりすることは難しく、現実的な方法ではなかった。

【0 0 0 7】

また、電子メールに関しては発送する側のコストが低いため、メールアドレスさえ知っていれば大量の電子メールを送ることができてしまう。このため、SPAMを、何らかの方法で、いずれから収集してきたメールアドレスに向かって一斉に送ることが容易に可能となっている。SPAMは、インターネットの普及率が高いアメリカなどでは大問題となっており、日本でも問題になりつつある。

【0 0 0 8】

本発明の課題は、悪戯メールの受信を防止することのできる装置及び方法を提供することである。

【0 0 0 9】

【課題を解決するための手段】

本発明の第1の側面における装置は、悪戯メールを防止する装置であって、受信した電子メールからメールアドレスを抽出するメールアドレス抽出手段と、特

定のメールアドレス、または、特定のメールアドレスパターンに対応して、該受信した電子メールの処理方法を登録する記憶手段と、該受信した電子メールのメールアドレスと該記憶手段に記憶されているメールアドレス、または、メールアドレスパターンとの照合を行い、該照合の結果得られた処理方法に基づいて、該受信した電子メールを処理するメール処理手段とを備えることを特徴とする。

【 0 0 1 0 】

本発明の第 2 の側面における装置は、電子メールを受信する受信手段と、受信した全ての電子メールに、送信元のアドレスを付加する手段とを備える電子メールサーバから電子メールを受信する装置であって、受信した電子メール中に含まれている、送信元のアドレスを解釈して、特定のメールアドレス、あるいは特定のメールアドレスパターンに対しての処理方法を設定する手段を備えることを特徴とする。

【 0 0 1 1 】

本発明の第 1 の側面における方法は、悪戯メールを防止する方法であって、（a）受信した電子メールからメールアドレスを抽出するステップと、（b）特定のメールアドレス、または、特定のメールアドレスパターンに対応して、該受信した電子メールの処理方法を登録するステップと、（c）該受信した電子メールのメールアドレスと該ステップ（b）で記憶されたメールアドレス、または、メールアドレスパターンとの照合を行い、該照合の結果得られた処理方法に基づいて、該受信した電子メールを処理するステップとを備えることを特徴とする。

【 0 0 1 2 】

本発明の第 2 の側面における方法は、電子メールを受信する受信手段と、受信した全ての電子メールに、送信元のアドレスを付加する手段とを備える電子メールサーバから電子メールを受信する方法であって、受信した電子メール中に含まれている、送信元のアドレスを解釈して、特定のメールアドレス、あるいは特定のメールアドレスパターンに対しての処理方法を設定するステップを備えることを特徴とする。

【 0 0 1 3 】

本発明によれば、電子メールサーバ側、あるいは、電子メールサーバから電子

メールを受信するクライアント側において、簡単な方法で、使い捨てのメールアドレスを作成したり、特定の相手専用のメールアドレスを作成したり、受信者には分からない暗号化された情報を含んだメールアドレスを作成することができる。従って、不本意な相手からのメールを簡単に見分けることができ、受け取りたいメールだけを簡単に受け取ることができるようになる。

【0014】

【発明の実施の形態】

図1は、本発明の第1の実施形態を示す図である。

同図(a)は、サーバの機能構成を示した図である。

【0015】

メール転送サーバ1（以下、サーバ1と記載）は、ある一定のフォーマットに該当するメールアドレスを全て特定の人に送るようにする。例えば、メールアドレスが

`ueda@xxxxxx.server.com`

あるいは、`ueda.xxxxxx@server.com`

のようなフォーマットのメールについて、該メールアドレス内の任意の「xxxxxx」に該当するメールに対して登録されたメールアドレスへの転送、もしくは該メールに対して登録された特定のメールボックスへの配送を行う。

【0016】

「xxxxxx」の部分に任意の長さの文字を許すようにすれば理論的に無限のメールアドレスが可能であり、十分に長い固定長の文字列を許すようにしても非常に多数のメールアドレスから一つのメールボックスへの配送ができる。

【0017】

このことにより、ユーザは自分が受け取ると決めた「xxxxxx」を含まないメールアドレスに対するメールを拒否／消去することが簡単にできるようになる。

通常の使用では、メールのユーザは自分にメールを出す可能性がある人に対してそれぞれ異なったメールアドレスを通知し、該通知した全てのメールアドレス以外のメールアドレスに届いたメールは捨てるか無視すればよい。

【0018】

このようにすれば、もしもあるメールアドレスがSPAMの対象になっていると分かった場合、それまで使っていたメールアドレスを単に使わなくするだけで良く、そのメールアドレスで送ってくるはずだった人がSPAMを出したか、SPAMを出す人にメールアドレスを漏らしたことが分かる。

【0019】

また、ホームページ上でニュースを掲載する場合などで、責任の所在を明確にするために自分のアドレスを公開しなくてはならない場合には、一通毎に異なったメールアドレスを用い、かつ、返事の中に特定のキーワードを書いてもらったメールについてのみ返事を受け付けるようにすれば、そのようにして知ったメールアドレスを集めてもSPAMを送ることはできなくなる。

【0020】

ユーザは、あらかじめサーバ1に対して受信するメールのアドレスの登録をし、該受信メールの送信先として、自分宛のメールアドレスを取得してあるものとする。このメールアドレスを仮に「name@server」とする。

【0021】

サーバ1は、無限個のメールアドレスを用意するために以下のどちらかを行う。

1) name部分に使わない文字(例えば「.」)を用いて「name. 任意の文字列@server」宛のメールを全て「name@server」宛のメールとして扱い、必要に応じて、再配布あるいは、メールボックスに入れる。

【0022】

2) Domain Name Service のMX (Media eXchange) フィールドを用いて「name@ 任意のドメイン名.server」宛のメールをサーバ1で受け取る旨を、世界中に通知し、その受け取ったメールを全て「name@server」宛のメールとして扱い、必要に応じて、再配布あるいは、メールボックスに入れる。

【0023】

更に、サーバ1は、メール受け付け部3において、送信されてきたメールのアドレスあるいはアドレスパターンの照合を行った後、メールを再配布あるいはメールボックスに入れる際に、前もって与えられたユーザからの指示に従って、メ

ールの破棄、エラーメールを送出することによるメールの拒否、あるいは、ユーザのメールリーダーソフトが処理できるような何らかのフィールドの追加などの処理をする。この何らかのフィールドの追加処理では、例えば、米国特許 5 3 7 7 3 5 4 号のような装置を使って、ユーザが容易に無視したり破棄したり、更には読む際の優先度を低くできるようにする。

【 0 0 2 4 】

ユーザは、サーバ 1 に対して、指示を行う際に以下のような処理を実施する手段のどれか一つ以上あるいは全てを持つ。

- ・ある特定のメールアドレスと処理方法を指定し、それ以降そのメールアドレスに届いたメールはその方法で処理する。
- ・ある特定のメールアドレスのパターンとその処理方法を指定し、それ以降そのパターンにマッチするメールアドレスに届いたメールはその方法で処理する。
- ・全てのメールアドレスに対して処理方法を指定し、それ以降の全てのメールはその方法で処理する。

【 0 0 2 5 】

このために、サーバ 1 の内部に、指定されたアドレスとそのアドレスに対応する処理方法とを対にして記憶する処理内容記憶部 2 を設ける。同図 (b) は、処理内容記憶部 2 に記憶されるテーブルの例である。このテーブル 2 a の 1 行は、アドレス又はアドレスパターンを格納するフィールド、該アドレス又はアドレスパターンに対応する処理方法を格納するフィールド、及び該処理方法に於いて使用される処理方法のパラメータなどを記憶するオプションを記憶するフィールドからなる。サーバ 1 は、届いたメールのアドレスをテーブル 2 a に登録されている指定されたアドレス、アドレスパターンと照合し、テーブル 2 a 内にマッチするアドレス、または、アドレスパターンが存在する場合、そのマッチしたアドレスあるいはアドレスパターンに対応する処理を行う。また、全てのメールアドレスに対して処理が指定されている時は、そのユーザへ届いた全てのメールに対して処理を行う。

【 0 0 2 6 】

サーバ 1 はまた、ユーザが処理方法の登録／参照を行うための入出力部 4 を有

しており、ユーザから、入出力部 4 を介して処理方法のリストの参照要求があった時は、そのユーザ名に対応する全ての処理方法のリスト（アドレスパターン、オプションを含む）をユーザに提示する。また、同じく、入出力部 4 を介するユーザからの処理方法の登録に際しては、

- ・古い登録の消去、
- ・登録内容の変更、
- ・新規の登録

を行う。

【0027】

アドレスパターンの検索の順序が意味を持つようにすることで、複数のアドレスパターンが一つの宛先に対してマッチする場合に前にあるパターンを優先的に使う事で曖昧性なく処理を実行できるようにすることができる。すなわち、マッチする範囲が狭いように指定できる様にする。これにより、例外的なパターンや、前に、一般的なパターンを後に指定できる様になる。この場合には、サーバ 1 は、ユーザから入出力部 4 を介して入力される、登録された処理方法の順位の変更（何番目にそのパターンを調べるか）要求、も受け付けるようにする。

【0028】

あるいは、曖昧な場合には登録を受け付けないようにしたり、あるいは、曖昧な場合にはサーバ 1 の方で適当にマッチする一つの処理方法を選んで処理するようにしても良い。

【0029】

図 2 は、上記構成のサーバ 1 により実行される検索の順序が意味を持つ場合の処理の一例を示す図である。

サーバ 1 が電子メールを受信し、メール受付部 3 においてアドレス、あるいは、アドレスパターンの照合を行った結果、その電子メールの信用度が曖昧である場合には、特定の処理を行うようにする。同図（a）は、サーバ 1 のメール受付部 3 がメール受信時に行う処理を示す図である。

【0030】

処理の方法としては、以下のどれか一つ、あるいは、全てを行う。

- ・通常通り配送を行う。
- ・単に配送をしない。

【0031】

配送処理をしないという処理方法に該当するアドレスにメールが届いた場合、この場合、サーバは何もしない。

同図（b）は、上記の場合に処理内容記憶部2に記憶されるテーブル2aの内容の例を示している。

【0032】

この場合、アドレス又はアドレスパターンのフィールドに、特定のアドレスあるいは、アドレスパターンを記憶し、対応する処理方法のフィールドには、「捨てる」という処理内容を記録する。オプションは特になしとしている。サーバ1は、該処理内容がテーブル2aに登録された電子メールを受信すると、同図（b）のテーブル2aを参照し、該当する処理方法を読みとって、上記電子メールを「捨てる」処理を行う。実際には、電子メールを配送せず、単に何もしなければ、電子メールがメールボックスから自動的に消えてしまう。

【0033】

図3は、受信した電子メールが所定のアドレスあるいはアドレスパターンに一致した場合にエラーメールを送出して拒絶するときのサーバ1の処理と、その場合に、処理内容記憶部2に記憶されるテーブル2aの内容を示す図である。

【0034】

同図（a）は、サーバ1のメール受け付け部3の処理を示した図である。

届いたメールのアドレスあるいはアドレスパターンが、テーブル2aに登録されている特定のアドレスあるいはアドレスパターンと一致した場合、サーバは通常の宛先不明のアドレスが見つかった場合と同様にエラーメールを作成し、それをメールの送付元に送りつける（エラーメール送出）。

【0035】

エラーメールは、実際に送受信中にエラーが発生したと同じように作成され、SPAMと思われるメールを受け取った時に、送信元に対して返送するため、SPAMの送信者に、メールを送った相手のアドレスが間違っていたなどと思わせ

る。

【0036】

同図（b）は、上記エラーメール送出处理を実現するためにサーバ1の処理内容記憶部2に記憶されるテーブル2aの内容例を示す図である。

特定のアドレスあるいはアドレスパターンに対して、処理方法として「エラーメール送出」を登録しておく。この例ではオプションは特に無しとしているが、エラーメッセージに含まれる言葉のオプションを登録しておき、エラーメッセージを生成する際に、これらの言葉のオプションから任意に選択して利用するようにすることも可能である。

【0037】

図4は、サーバ1が通常のようにメールは配送するが、メッセージ中に指定された目印を加える処理を行う場合のメール受け付け部3の処理、処理方法記憶部2のテーブル2aの登録内容及び目印の例を示した図である。

【0038】

同図（a）は、サーバ1のメール受け付け部3の処理を示す図である。

処理方法として「目印の付加」を指定する場合は、どんな目印を付加するかユーザが指定する。指定された目印はサーバ1の処理方法のオプションとして処理内容記憶部2に記憶される。従って、同図（b）に示されるように、処理方法記憶部2に記憶されるテーブル2aには、特定のアドレスあるいはアドレスパターンに対応して、メールに目印を付加する処理方法を採用することが登録されると共に、オプションのフィールドに目印の付加方法（どのようなメッセージを付加するかに関する情報）が登録される。

【0039】

この処理方法に該当するアドレスのメールが届いた場合、サーバ1は、届いたメールに対して、指定された目印を加えた後、通常のメールと同様の配送を行う。

【0040】

同図（c）は、目印の付け方の一例を示した図である。

同図では、メール5のヘッダ部5aに“X-possibly-spam:true”という目印を

付ける例を示している。このようにすることによって、ユーザは、届いたメールがSPAMであるか否かを判別することができる。また、このメッセージを元に、クライアント側で、当該メールを破棄するようにしても良い。目印の付け方は、従来の項で参照した文献を参照されたい。従って、詳細は省略する。

【0041】

図5は、サーバ1が通常のようにメールは配送するが、届いたメールアドレスをメッセージ中に加える場合の処理手順、テーブル2aの内容、処理例を示した図である。

【0042】

同図(a)は、サーバ1のメール受け付け部3の処理を示す図である。また、同図(b)は、処理内容記憶部2に記憶されるテーブル2aの内容例を示す図である。

【0043】

同図(b)に示すように、届いたメールのアドレスの処理方法として送付宛先を付加する処理が指定されている場合、サーバ1は、その届いたメールに対して、例えば、ヘッダ部分の決まったフィールドに、

X-Forwarded-From: 届いたアドレス

のような形式でアドレスを追加した後、通常のメールと同様の配送を行う。

【0044】

同図(c)は、メール6のヘッダ部分6aに上記形式でメールを送信してきた相手のアドレスを書き込んで送付先のクライアントへ該メール6を送信する処理形態を示した模式図である。

【0045】

同図(a)に示されるように、サーバ1のメール受け付け部3は、メールを受け取ると、そのメールの送り主のアドレスを同図(b)のテーブル2aに登録されているアドレスあるいはアドレスパターンと照合し、一致しない場合には、通常のメール処理を行うが、一致した場合には、テーブル2aの一致した行の処理方法のフィールド及びオプションのフィールドを参照して、処理を決定する。今の場合、処理方法は、「送付宛先を付加」であり、オプションは「なし」なので

、メールのヘッダ部などの予め決められた部分に上記したようなメッセージを添付してクライアントに送付する。クライアントは、受信メールのこの予め決められた部分に記載されている送り主の記載を見て、破棄するなり、受信することができる。送り主のアドレスを参照して、そのメールを破棄するかしないかを自動的に判断し、当該処理を実行するプログラムをクライアント側に設けておくことも可能である。

【0046】

同図(c)の例では、メール6のヘッダ部6aに「X-Forwarded-Form: ueda.xx.xxx@fuji」が添付されている。添付のための具体的な処理方法は、従来の技術の項で参照した文献を参照されたい。従って、詳細は省略する。

【0047】

図6及び図7は、届いたメールが特定の性質を持ったものかどうか判定し、それによってメールの処理方法を指定するサーバ1の処理手順と処理方法の記録例を示す図である。

【0048】

この処理方法を指定する場合は、処理方法記憶部2のテーブル2aに、見分けるべき性質の記述、その性質を持っている場合と持っていない場合の処理方法が登録される。見分けるべき性質と、該性質を持っている場合と持っていない場合の処理方法はオプションとしてテーブル2aに記憶される。あるいは、サーバ1の振る舞いを一部固定して、上記性質を持っているメールの場合は何もしないで破棄し、持っていないメールの場合は送り主のアドレスを該メールに記載し、処理方法では性質だけを指定させ、具体的な処理は、サーバ1にオプションとして記憶させるようにしても良い。

【0049】

見分けるべき性質は、さまざまなものが考えられるが、メールに関する各種情報のパターンマッチ、例えば、Subjectが特定の文字列を含むとか、送出した日付が一定の期間内にあるかどうか、あるいは、本文中に特定の文字列が含まれるかどうかなどが考えられる。

【0050】

この処理方法に該当するアドレス宛のメールが届いた場合、サーバ 1 のメール受け付け部 3 は、そのアドレスに対応した見分けるべき性質を取り出し、次にそのメールが特定の性質を満たしているかどうか調べ（ステップ S 1 0 : 図 6 及び図 7）、性質を満たされているか否かを判断する（ステップ S 1 1 : 図 6 及び図 7）。次に、満たしている場合は、そのための処理を（ステップ S 1 2、S 1 2'）、そうでなければそうでない方の処理を（ステップ S 1 3、S 1 3'）、処理方法記憶部 2 のテーブル 2 a のオプション・フィールドあるいはサーバ 1 の固定情報記憶域から取り出し、該当する処理を行う。この処理の方法は、前述した処理方法のいずれであっても良いし、サーバ 1 によっていくらか制限を加えても良い。あるいは、後述するような処理でも良い。

【 0 0 5 1 】

図 8 及び図 9 は、処理方法を暗号化してメールアドレスの任意文字列の中に埋め込んでおき、サーバ 1 はそれを解釈して実行する場合のサーバ 1 の処理手順とサーバ 1 に記憶されるデータを示す図である。

【 0 0 5 2 】

図 8 (a) 及び図 9 (a) は、サーバ 1 の処理手順を示す図であり、図 8 (b) は、暗号解読用の鍵を記憶するテーブル 4 であり、図 8 (c) 及び図 9 (b)、(c) は、処理方法記憶部 2 のテーブル 2 a の内容例を示す図である。

【 0 0 5 3 】

ユーザはこの処理方法を指定する前に暗号解読の鍵をサーバ 1 に登録する。鍵はサーバ 1 の種類に応じて、ユーザ毎に指定するようにしても良いし（図 8 (b) 参照）、アドレスパターン毎に変えるようにしても良い。すなわち、前者ではユーザ毎のオプションとして暗号解読の鍵を保存し（図 8 (b)）、後者では処理方法のオプションとして鍵を保存する（図 8 (c)）。

【 0 0 5 4 】

また、ユーザがこの処理方法を指定する場合、暗号化されたコマンド部分を取り出すためのパターンを指定し、それはオプション、アドレスパターンの一部、またはオプションの一部もしくは処理方法の一部としてサーバ 1 内部のテーブル 2 a に保存される（図 9 (b)、(c)）。

【0055】

ユーザはメールアドレスを知らせる際に処理すべきコマンドをサーバ1が解釈できるような文字列で表現し、次にその文字列を暗号化する。そして、該暗号化されたコマンドとこの処理方法を、指定したアドレスパターンに適合するような形式にして、メールアドレスの任意の文字列の部分に加えて、最終的にメールアドレスを作成し、このメールアドレスをサーバ1に知らせる。

【0056】

サーバ1のメール受け取り部3は、この処理方法に該当するアドレスにメールが届いた場合（ステップS15で、照合した結果、一致を見た場合）、まず、内部に保存された暗号化されたコマンド部分を取り出すためのパターンを取り出し、それに従って、上記アドレスから暗号化されたコマンド部分を取り出す（ステップS16）。そして、そのコマンド部分を入出力部4内に予め保存されている当該鍵を用いて解読し（ステップS17）、次に解読された文字列（コマンド）を解釈して処理を行う（ステップS18）。処理は上述されたどの方法をとっても良いし、サーバによっていくらかの制限を加えても良い。また、サーバによっては適当なプログラミング言語（例えば、Perl）の処理系と連係することにより高度の処理を行っても良い。

【0057】

また、図5のサーバ1は、常に全てのメールアドレスに対してメールを配送し、予め、テーブル2aに登録されている該当アドレスのメールについては、届いたメールアドレスをメッセージ中に加えるという操作をするが、サーバ1にこのような機能を持たせつつ、入出力部4からの指示を一切受け付けなくようにすることもできる。このようにすると、メールアドレスによって処理方法を変える必要がないので、サーバ1の方でユーザの指定方法を受け付ける構成要素とアドレスあるいはアドレスパターン毎に行う複雑な処理が不要となり、サーバ1の負荷を大幅に減らすことができる。

【0058】

なお、理論的に無限通りのアドレスを一つのアドレスに対応させ、メールを届けることは既知の技術であるが、届いたアドレスをメール内に付加することで、

悪戯メールに対処できるようにすることが本願の新しい技術である。

【 0 0 5 9 】

前述の説明では、サーバ 1 に処理をさせていたが、サーバ 1 を使ったのと同じ効果を得るのに、負荷の重いサーバでなくクライアント側で処理を行うような構成にすることも可能である。また、あらかじめ暗号鍵を公共の通信路を通して送るのは危険であるが、クライアントに暗号鍵など上記暗号化の処理に必要な情報を全て置くことでこの危険をなくすることができる。

【 0 0 6 0 】

図 1 0 は、クライアントに悪戯メール防止装置を設ける場合のサーバの処理を説明する図である。

この場合、サーバ 1 0 は、メールを受信すると、メールの送り相手のアドレスをメール内の、例えば、ヘッダ部に記録した後、通常のメール処理を行う。通常のメール処理とは、受信メールのクライアントへの配信などである。

【 0 0 6 1 】

クライアントで処理をする場合は、サーバで行う「通常のメールと同様の配送を行う」処理を、クライアント側で「通常のメールと同様に表示する」処理に置き換えて実行するようにする。

【 0 0 6 2 】

図 1 1 は、クライアント側で悪戯メールの処理を実行する場合のクライアントの構成を示す図である。

まず、クライアント 2 0 は、メールを取り込むと、そのアドレスを見て、処理方法記憶部 2 2 内のテーブル 2 2 a に記憶されているアドレスあるいはアドレスパターンと一致するか否かを判断する。一致しない場合には、メール表示／作成装置 2 1 において、メールの表示を行う。また、照合の結果、一致した場合には、処理方法記憶部 2 2 に記憶されているテーブル 2 2 a の処理方法、オプションの各フィールドを参照して、前述したサーバ 1 と同様な処理を行う。メールを作成する場合には、ユーザがメール表示／作成装置 2 1 を使用して作成する。このとき、処理方法記憶部 2 2 内のテーブル 2 2 a を参照して、テーブル 2 2 a に登録された相手にメールを送信する場合には、暗号化したパターンを含んでいるア

ドレスを送信相手に教えるための処理を行う。

【0063】

更に、クライアント20の付加機能として、相手が自分にメールを送信するときに発行した自分のアドレスを付加的な情報（発行日時、発行した相手、その他）と関連づけて記録しておくことで、届いたメールのアドレスに対応したそれらの情報を表示するようにすることもできる。このために、付加的情報の表示装置23が設けられると共に、処理方法記憶部22内のテーブル22aには、各アドレスあるいは各アドレスパターンに対応して、日時や相手の名前などを記録できるようにしておく。これにより、どのような相手からメールアドレスが漏れたのか、事後に調査することが容易に行える。

【0064】

更に、クライアントの付加機能として、発行したアドレスに対して受け取れる相手を関連づけて記録しておくことで、その後そのような相手にメールを出す際には記録されている発行したアドレスを差出人として自動的に用いるようなクライアントを実現することができる。

【0065】

このために、処理方法記憶部22内のテーブル22aのアドレス部（アドレスのフィールド）にパターンでなく特定のアドレスを登録できるようにし、テーブル22a内にオプションとして、受け取りたい相手のメールアドレス（の列）を保存するようにする。

【0066】

メールを作成する際には、送る相手のアドレスと一致するアドレスを受け取りたい相手として持つようなアドレスパターンをテーブル22aから検索し、見つければそれを差出人として使う。複数の相手に同時にメールを送る場合には、それらの送り先全てを受け取りたい相手として持つようなアドレスパターンをテーブル22aから検索する。

【0067】

もしも見つからなければ、新しい相手先（あるいはその組み合わせ）なので、以下の1）～3）どれかをユーザに選ばせるか、あるいはシステムが1）～3）

の中のいずれかを固定的に選んで動作する。

- 1) デフォルトのアドレスを使う、
- 2) 既存のアドレスパターンのどれか一つを用いる、
- 3) 新しいアドレスを作り、それと新しい相手先を関連づける。

【0068】

2) の動作をする場合には、相手先（の全て）をそのアドレスパターンの受け取りたい相手としてテーブル 2 2 a に登録することができる。

また、受け取りたい相手以外からのメールを別処理するように構成しても良い。この場合、該別処理としては、処理方法記憶部 2 2 内のテーブル 2 2 a のオプション部（オプション・フィールド）に指定された動作、あるいは、クライアント 2 0 で固定された動作（例えば、そのメールを捨てる）等が考えられる。

【0069】

あるいは、図 1 2 に示されるように、クライアント 2 0 がエラーメールと同等の内容のメールを作成し（ステップ S 3 1）、これを送り主に送り返すようにする（ステップ S 3 2）ことも可能である。

【0070】

以下に、サーバ 1 側で悪戯メールを処理する場合のサーバ 1 の機能の具体例を説明する。

サーバ 1 は内部に登録された処理方法のリストを持っている（図 1（a）の処理内容記憶部 2 及び図 1（b）のテーブル 2 a 参照）。処理方法のリストはアドレス部（アドレス又はアドレスパターン）、処理方法、オプション部の 3 つが一組となった情報のリストである。アドレス部は正規表現を用いたパターンで表されるものとし、特定アドレスへのマッチを希望する時には、ワイルドカード文字を使わず、また、全てのアドレスにマッチを希望する時には「ユーザ名、＊」のパターンを保持する。

【0071】

ただし、以下のような制限が課せられてあるものとする。

図 4 の場合は目印はメールのヘッダ部にのみ付加できるものとし、該目印として付加すべきヘッダの文字列を登録する。

【0072】

図6あるいは、図7の場合においては、区別する性質は、メールのヘッダ部の正規表現を用いたパターンマッチとし、見るべきヘッダフィールド名、マッチするパターン（正規表現）、そして、マッチした場合とそうでない場合の処理の内容が再帰的に指定できるものとする。この場合、再帰的な処理内容のオプション部も同時に指定できるものとする。

【0073】

図8及び図9の場合の暗号鍵は処理方法毎に異なっていて良いものとし、これを処理内容記憶部2のテーブル2aのオプション部に記憶する。また、テーブル2aのアドレス部に一組の括弧をいれることで、それらで括られた部分を暗号化されたコマンドとして扱うことを示すものとする。サーバ1は復号化されたコマンドの解釈・実行により「メールを処理する」サブプログラム（メール処理サブプログラム）を呼び出すようにする。

【0074】

サーバ1は、メールを受け取った場合、「user. 任意の文字列@server.domain」というメールアドレスを全て「user@server.domain」というメールアドレスに届いたものとして扱うものとする。

【0075】

サーバ1はメールを受け取ると、宛先アドレスを「宛先」として記憶し、また「@」より左側の文字列を「拡張ユーザ名」として記憶する。また、拡張ユーザ名の最も左にある「.」よりも左側の文字列を取り出し、この文字列を「ユーザ名」として記憶する。もしも、メールアドレスに「.」が含まれていなければ拡張ユーザ名と同じ文字列を「ユーザ名」として記憶する。

【0076】

次に、拡張ユーザ名と、処理方法のリストの各アドレス部とを順に照合し、マッチするかどうか調べる。

もしもどれともマッチしなければ、「ユーザ名@server.com」宛のメールとして、通常の配送処理を行う。

【0077】

もしもどれかとマッチした場合、そこに記述された処理方法とオプションに従って、メールを処理する。

<メール処理サブプログラムのアルゴリズム>

メール処理サブプログラムの呼び出し形式は、次の通りである。括弧内は引数。

【0078】

サブプログラム：メールを処理する（処理方法、オプション、メール、拡張ユーザ名、ユーザ名、宛先）

メール処理サブプログラムの機能は、次の通りである。

- ・処理方法が、「mail」の場合、「ユーザ名@server.com」宛のメールとして、通常の配送処理を行う。

- ・処理方法が、「dispose」の場合、単にそのメールを捨てて処理を終了する。

- ・処理方法が、「error」の場合、通常処理の中の宛先不明の場合のエラーメール送付のルーチンに行き、該ルーチンの実行によりエラーメールを送出する。

- ・処理方法が、「header」の場合、オプション部に記憶されている、目印の文字列をメールのヘッダ部に付け加え、「ユーザ名@server.com」宛のメールとして、通常の配送処理を行う。

- ・処理方法が、「mark」の場合、メールのヘッダ部分に

X-forwarded-from：宛先

という文字列をつけ加え、「ユーザ名@server.com」宛のメールとして、通常の配送処理を行う。

- ・処理方法が、「if」の場合、オプション部は以下の項目がつながった文字列であるとする。

- ・（）で括られた調べるべき性質

- ・{}で括られている、上の性質を満たしたときの処理方法とオプション

- ・{}で括られている、上の性質を満たさないときの処理方法とオプション

調べるべき性質には、以下のいずれかあるいは、それらを&&、||、またはつりあった（）で括って任意個連結したものとする。

- ・フィールド名：受理パターン

- ・フィールド名！非受理パターン
- ・date before 日付
- ・date after 日付

ただしパターンは正規表現とする。

【 0 0 7 9 】

フィールド名はメールのヘッダ部にあるフィールド名で例えばFromあるいは、Subject のようなものである。

処理方法とオプションは、メール処理サブプログラムで処理できる処理方法とそのオプションが空白で区切られて並んでいるものとする。ただしオプションがない場合には空白がない場合を許可する。

【 0 0 8 0 】

まず、オプション部から以上のフォーマットされた文字列から調べるべき性質を取り出し、それに従って届いたメールのヘッダを調べる。

調べるべき性質が「フィールド名：受理パターン」の場合は、メールからそのフィールド名の内容をメールから取り出しそれが受理パターンとマッチする場合のみ真となりそれ以外は偽となる。

【 0 0 8 1 】

調べる性質が「フィールド名！非受理パターン」の場合は、メールからそのフィールド名の内容をメールから取り出しそれが受理パターンとマッチしない場合のみ真となりそれ以外は偽となる。

【 0 0 8 2 】

調べるべき性質が「date after 日付」の場合は、メールのDateフィールドを解釈し、また「日付」部分の日付を解釈しDateフィールドの日付が指定の日付より後の場合のみ真となりそれ以外は偽となる。

【 0 0 8 3 】

調べるべき性質が「date before 日付」の場合は、メールのDateフィールドを解釈し、また「日付」部分の日付を解釈しDateフィールドの日付が指定の日付より前の場合のみ真となりそれ以外は偽となる。

【 0 0 8 4 】

調べるべき性質が「date before 日付」の場合は、メールのDateフィールドを解釈し、また「日付」部分の日付を解釈しDateフィールドの日付が指定の日付より前の場合のみ真となりそれ以下は偽となる。

【0085】

調べるべき性質が&&、||、()で結合されている際には、&&は論理積、||は論理和で論理積の結合力が強いものとして扱い、()は通常と同じように優先的に結合して計算するようにして調べる。

【0086】

次に、調べた結果の真偽によって、二つの処理方法を選ぶ。処理方法から最初の空白まで（あるいは空白が無ければその全て）を処理方法とし、残りをオプションとして、再帰的にメール処理サブプログラムを呼び出す。

【0087】

例えば、オプション部には以下のような記述が可能である。

```
(Subject:.Hello.* &&From!friendname@some.domain) [if(From: spammer) [error] [header greeting:true]] [mail]
```

この場合、メールのSubject がHello を含みFromがfriend_name@some.domain を含まない場合は、ifで始まる部分が処理方法となり、再帰的にifの処理が行われる。それ以外の場合は通常のメール配送処理が行われる。

・処理方法が、「decrypt」の場合、まず、アドレスパターンの括弧で括られた部分とマッチする文字列を取り出し、この文字列を「暗号化されたコマンド」とする。次にオプション部から暗号の鍵を取り出し、この鍵を用いて暗号化されたコマンドを復号化する。そして、得られた文字列のうち、最初の空白までを処理方法、残りをオプションとしてメール処理サブプログラムを再帰的に呼ぶとする。

<処理方法のリストの登録／参照>

サーバ1はまた、処理方法のリストの登録／参照手段（図1（a）の入出力部4）を持っており、ユーザから、処理方法のリストの参照要求があった時は、そのユーザ名に対応する処理方法、すなわち「ユーザ名」というアドレス、あるいは「ユーザ名。」で始まるパターンを持った全ての処理方法のリスト（アドレス

パターン、オプションを含む) をユーザに提示する。

【0088】

処理方法の登録に際しては、

- ・古い登録の消去
- ・登録された処理方法の順位の変更 (何番目にそのパターンを調べるか)
- ・登録内容の変更
- ・新規の登録

が行えるようになっている。

<処理方法の登録>

サーバ1は、アドレス名、(サーバ1が解釈できる) コマンド、コマンドのオプションを受け取って、これらをユーザの登録された処理方法のリスト (図1 (a) の処理内容記憶部2のテーブル2a) に加える。

【0089】

具体例

- ・add アドレス コマンド名 [オプション]

コマンド名は “dispose ”、“error ”、“mark”、“header”、“if”、“decrypt ”、“mail” のどれかを使用する。

【0090】

アドレス、コマンド名、オプションは空白で区切られ、それらをサーバ1は分離して、文字列としてユーザにより登録された処理方法のリストとしてテーブル2aに記憶する。

【0091】

ユーザ指定の処理方法がすでにあるときは、新たに追加されたものはリストの最後に置く。

“dispose ”、“error ”、“header” はオプションを持たない。

【0092】

“mark” コマンドは付加ヘッダ名をオプションとして持つので、サーバ1は以下のようなコマンドを受け付ける。

add アドレス mark ヘッダ名 ヘッダ内容

(例えば、`add ueda.broadcast mark X-Possibly-Spam: true`)
を受け付け、ヘッダ名 (X-Possibly:) とヘッダ内容 (true) を文字列としてつな
げて、これをオプション部として扱う。

【0093】

“if” コマンドはチェック内容とその後の動作をオプションとして与える。オ
プション文字列は、メール処理サブプログラムのオプション部で受け付けられる
構文とする。

【0094】

非合致時の動作内容は省略でき、その場合、デフォルトとしてerror コマンド
が指定されたものとして、オプション文字列に加えてテーブル 2 a に記憶する。
合致時の動作内容も省略でき、その場合デフォルトとしてmailコマンドが指定さ
れたものとしてテーブル 2 a に記憶する。ただし非合致時の動作を指定するとき
は合致時の動作内容は省略できない。

【0095】

登録時の構文は、add のコマンドとオプションを合わせたものである。

サーバ 1 が受け取るコマンドは、例えば、以下ようになる。

```
add ueda.from.friends if (From: friend1@his.domain | From: friend
2@her.domain )
```

```
add ueda.1 month.from.990401 if (date before 1999/5/1) {mail} {
error }
```

```
add ueda.report if (Subject : .*bug.*report*) {if (From: customer
1 | From: customer2 ) {mark X-customer-report : yes } {mark X-bug-re
port: yes } } {mail}
```

サーバ 1 はこれらのコマンドを受け取り、オプション部分の全ての文字列をユ
ーザの指定として加える。

【0096】

“decrypt ” コマンドはアドレスパターン中に \ (\) で括られた複合可能部
分を含むパターンを指定し、その他にオプションとして復号鍵を受け取る。

パターンの正規表現は通常と異なり、“.”、“*”は\でエスケープされて

いる場合、初めてワイルドカード文字として扱われる。

【0097】

サーバ1が受け取るコマンドは例えば下記のようになる。

add ueda.commandkey1.\ (\. * \) decrypt Nsa0ghzaldvaJAgalAsfD03

4J

復号化された文字列はadd のコマンドとオプションを合わせた文字列である。

＜処理内容の参照＞

ユーザ名を与えてその登録された処理方法のリストを返す。

【0098】

具体例

show ユーザ名

をサーバ1に送ると、ユーザ名. で始まる登録された処理方法のリストの内容を全てテキストで送り返す。

【0099】

送り返される内容は、登録時の構文の内、add を除いたアドレスパターン以降のフォーマットとする。

＜処理内容の消去＞

アドレスパターンを与えて、それと全く同じ内容のパターンを検索し、相当する項目をリストから消去する。もしも見つからなければエラーを返す。

【0100】

具体例

delete パターン

パターンと完全に一致する項目がテーブル2 a 内にあれば、その項をテーブル2 a から消去し、消去する前の内容をshowと同様にテキストで送り返す。もしも見つからなければ、その旨のエラーメッセージをテキストで送り返す。

＜処理内容の変更＞

アドレスパターンとそこでの変更内容であるコマンド（とそのオプション）を与えて、現在登録されている処理方法と入れ替える。

【0101】

具体例

replace パターン コマンド名[オプション]

構文はadd コマンドと全く同じである。パターンと完全に一致する項目があれば、その項のコマンドとオプションを変更処理で指定されたコマンド名とオプションで入れ替える。そして、入れ替える前の情報をdeleteと同様にテキストで送り返す。もし、パターンが見つからなければ、add と全く同じに動作し、元のパターンが見つからなかった旨の警告をテキストで送り返す。

＜変更処理の内、順序入れ替えに関するもの＞

アドレスパターンとそのパターンを検査する順序を指定し、その指定された順序に指示パターンを移動させる。

【0102】

具体例

order パターン 順番

パターンと完全に一致する項目があれば、その項を前から数えて指定された順番で検査されるように、指定のリストの順序を変更する。この変更によって、それ以降の検査は一つずつ検査の順序が後ろにずれるようにする。もしも一致する項目がなければ、パターンが見つからなかった旨のエラーをテキストで送り返す。

＜メールアドレス作成部（クライアント20にある独立したプログラム）＞

メールの作成で暗号化する場合、

クライアント20のプログラムは、ユーザに対して、チェックするフィールド名又は日付を問い合わせる。図13は、クライアント20のプログラムが、ユーザにフィールド名や日付を問い合わせるユーザ・インタフェース画面30のフォーマットの一例を示している。

【0103】

これに従い、非受理のボタン31がチェックされていたら、

フィールド名！パターン&&

受理のボタン32がチェックされていたら、

フィールド名：パターン&&

日付のfromフィールド35に入力があれば、

Date from 日付

日付のtoフィールド36に入力があれば、

Date after 日付

を文字列にしてつなげコマンドとする。

【0104】

Subject,to,From に対応して、パターン37～39を使用する。

＜サーバとクライアントの組み合わせ＞

上記説明では、サーバ1が悪戯メールの処理を行う主旨で説明したが、前述したように、クライアント20側で悪戯メールの処理を行うことも可能である。この場合、図10のサーバ10と、例えば図11のような、図2～図9のサーバ1の機能を有したクライアント20とを組み合わせることができる。

【0105】

サーバ10はメールを受け取ると、メールアドレスの「@」より左側の文字列を調べ、メールアドレス内に「.」が含まれていなければ通常の配送処理（ユーザ名不明の場合のエラーメール送出を含む）を行う。一方、「.」が含まれていなければ、宛先のアドレスを「宛先」として記憶し、また、最も左にある「.」よりも左側の文字列を取り出し、それを「ユーザ名」として記憶する。

【0106】

そして、受信メールのヘッダ部分に、例えば、

X-Forwarded-From: 宛先

という文字列を付け加え、「ユーザ名@server.com」宛のメールとして、通常の配送処理を行う。X-Forwarded-Fromという部分は、クライアントが処理できさえすれば、どのような文字列に変更しても良い。

【0107】

クライアント20（図11参照）に存在するメール表示／作成装置21は、前述の例と同様に処理方法のリストを持っているものとする。ただし、クライアント20の場合では更に、各々の登録されたアドレスに関する補助的な情報（例えば、最初に登録した日時、相手の氏名その他覚書）や相手として用いるアドレス

を蓄えることができるものとする。また、通常の処理として、メールの表示あるいはフォルダへの保存、破棄、作成（発送）を行えるものとする。

【 0 1 0 8 】

クライアント 2 0 はサーバ 1 0 からメールを受信すると、その中の X-Forwarded-From : 宛先というヘッダに注目し、その宛先を用いて、上記の例と同様の処理をする。ただし、上述したサーバにおける「通常の配送を行う」処理に関しては、クライアント 2 0 では、通常の処理の一部として、メールの表示あるいはフォルダへの保存を行うものとする。

【 0 1 0 9 】

エラーメールの配送に関しては、クライアントは通常そのような機能を有する手段を持たないので、標準的なエラーメールのフォーマットを内部的に保持しておき、それを用いて、エラーメールの送出を行うものとする。

【 0 1 1 0 】

クライアント 2 0 はまた、処理方法のリストの登録／参照手段（不図示、図 1 の入出力部 4 に対応する手段）を持っており、ユーザから、処理方法のリスト（処理方法記憶部 2 2 に記憶されているテーブル 2 2 a の登録内容）の参照要求があった時は、全ての処理方法のリスト（アドレスパターン、オプション、補助情報を含む）をユーザに提示する。

【 0 1 1 1 】

処理方法の登録に際しては、

- ・ 古い登録の消去
- ・ 登録された処理方法の順位の変更（何番目にそのパターンを調べるか）
- ・ 登録内容の変更
- ・ 新規の登録

が行えるようになっている。

【 0 1 1 2 】

クライアント 2 0 はまた、通常のメールの作成にあたり、処理方法の中にワールドカード文字を使っていないアドレスパターンに対応した相手のアドレスが登

録されている時には、そのアドレスパターンを差出人のアドレスとして使うようにすることができる。

【0 1 1 3】

このために、送る相手のアドレスと一致するアドレスを処理方法の受け取りたい相手として持つようなアドレスパターンを検索し、見つければそれを差出人として使う。複数の相手に同時にメールを送る場合には、送り先全てを受け取りたい相手として持つようなアドレスパターンを検索する。

【0 1 1 4】

もしも見つからなければ、新しい相手先（あるいはその組み合わせ）なので、以下のどれかをユーザに選ばせる。

- 1) デフォルトのアドレスを使う、
- 2) 既存のアドレスパターンのどれか一つを用いる、
- 3) 新しいアドレスを作り、それと新しい相手先を関連づける。

【0 1 1 5】

2) の動作をする場合には、相手先（の全て）をそのアドレスパターンの受け取りたい相手として登録するかどうか、更にユーザに問い合わせをすることで、次回からメールを送る際に同じ作業をしないようにできる。

【0 1 1 6】

【発明の効果】

以上、説明したように、本発明によればサーバ側が簡単な方法で無限ないし大量のメールアドレスを有するメールを一つのメールボックスへ配送するようにしたので、使い捨てのメールアドレスを作成したり、特定の相手専用のメールアドレスを作成したり、受信者にしか分からない暗号化された情報を含んだメールアドレスを作成することにより、不本意な相手からのメールを簡単に見分けることが可能となる。

【0 1 1 7】

この結果、SPAMと呼ばれる悪戯や宣伝のためのメールを簡単に除外して受け取りたいメールだけを簡単に受け取ることができるようになる。

また、このような機能をサーバとクライアントの組み合わせで行う様にするこ

とにより、サーバの改造をほとんど必要とせずに、現在流通している枠組みのサーバにおいても簡単に実現することが可能である。

【0 1 1 8】

また、SPAMメールを除外するのはサーバでもクライアントのソフトでも容易に行うことができ、かつ必要なメールは決して削除されない。

【図面の簡単な説明】

【図 1】

本発明の第 1 の実施形態を示す図である。

【図 2】

受信したメールの信用度が曖昧である場合の処理のサーバにおける処理の一例を示す図である。

【図 3】

受信した電子メールが所定のアドレスあるいはアドレスパターンに一致した場合にエラーメールを送出して拒絶するときのサーバの処理と処理内容記憶部に記憶されるテーブルを示す図である。

【図 4】

サーバが通常のようにメールは配送するが、メッセージ中に指定された目印を加える処理を行う場合のメール受け付け部の処理、処理方法記憶部のテーブル及び目印の例を示した図である。

【図 5】

サーバが通常のようにメールは配送するが、届いたメールアドレスをメッセージ中に加える場合の処理内容、テーブル、処理例を示した図である。

【図 6】

届いたメールが特定の性質を持ったものかどうか判定し、それによってメールの処理方法を指定するサーバの処理と処理方法の記録例を示す図（その 1）である。

【図 7】

届いたメールが特定の性質を持ったものかどうか判定し、それによってメールの処理方法を指定するサーバの処理と処理方法の記録例を示す図（その 2）であ

る。

【図 8】

処理方法を暗号化してメールアドレスの任意文字列の中に埋め込んでおき、サーバはそれを解釈して実行する場合のサーバの処理と記憶されるデータを示す図（その 1）である。

【図 9】

処理方法を暗号化してメールアドレスの任意文字列の中に埋め込んでおき、サーバはそれを解釈して実行する場合のサーバの処理と記憶されるデータを示す図（その 2）である。

【図 1 0】

クライアントに悪戯メール防止装置を設ける場合のサーバの処理を説明する図である。

【図 1 1】

クライアントで悪戯メールの処理をする場合のクライアントの構成を示す図である。

【図 1 2】

エラーメールと同等の内容のメールを作成し、これを送り主に送り返す場合の処理を示す図である。

【図 1 3】

クライアントのプログラムが、ユーザにフィールド名や日付を問い合わせるフォーマットの一例を示す図である。

【符号の説明】

- 1、1 0 サーバ
- 2 a、4、2 2 a テーブル
- 2 処理内容記憶部
- 3 メール受け付け部
- 4 入出力部
- 6 メール
- 6 a ヘッダ部

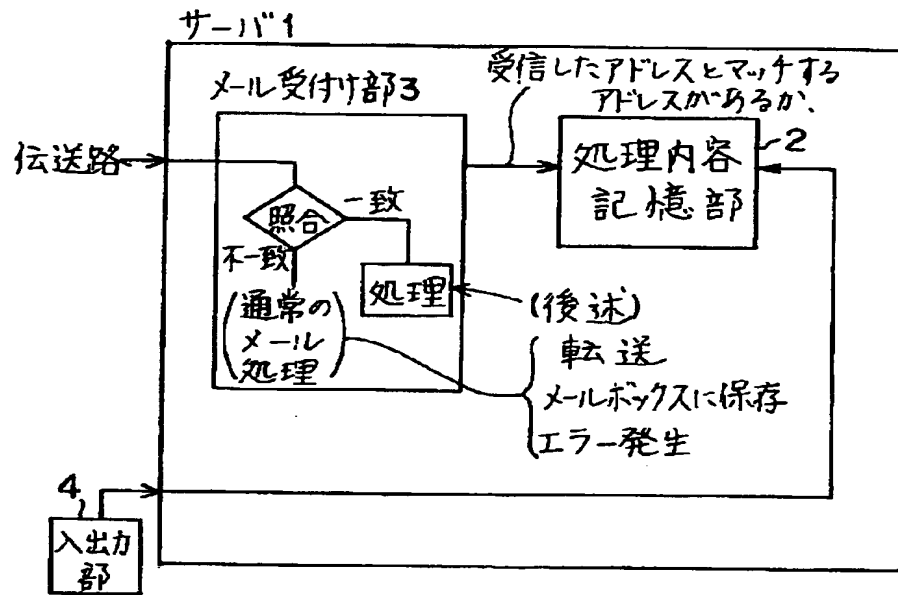
- 2 0 クライアント
- 2 1 メール表示／作成装置
- 2 2 処理方法記憶部
- 2 3 付加的情報の表示装置
- 3 0 ユーザ・インタフェース画面
- 3 1 非受理ボタン
- 3 2 受理ボタン
- 3 5 from入力フィールド

【書類名】

図面

【図 1】

本発明の第1の実施形態を示す図



処理方法の登録/参照

- ・参照
- ・追加
- ・変更
- ・消却

(a)

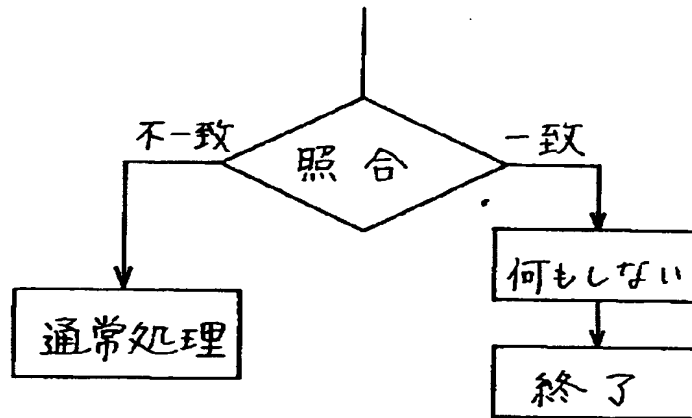
2a

アドレス又は パターン	処理方法	アクション

(b)

【図 2】

受信したメールの信用度が曖昧である場合の
処理のサーバにおける処理の一例を示す図



(a)

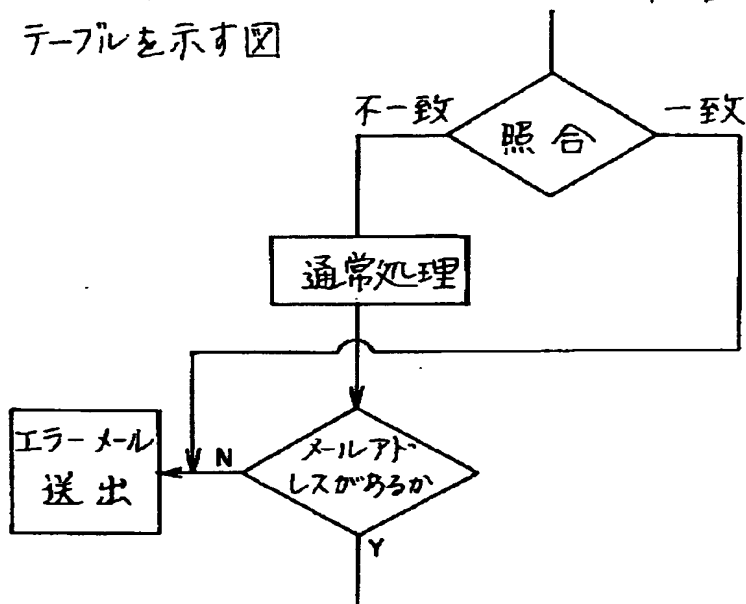
2a
↓

アドレス 又は パターン	処理方法	オプション
	捨てる	なし

(b)

【図 3】

受信した電子メールが所定のアドレスあるいはアドレスパターンに一致した場合にエラーメールを送出して拒絶するときのサーバの処理と処理内容記憶部に記憶されるテーブルを示す図



(a)

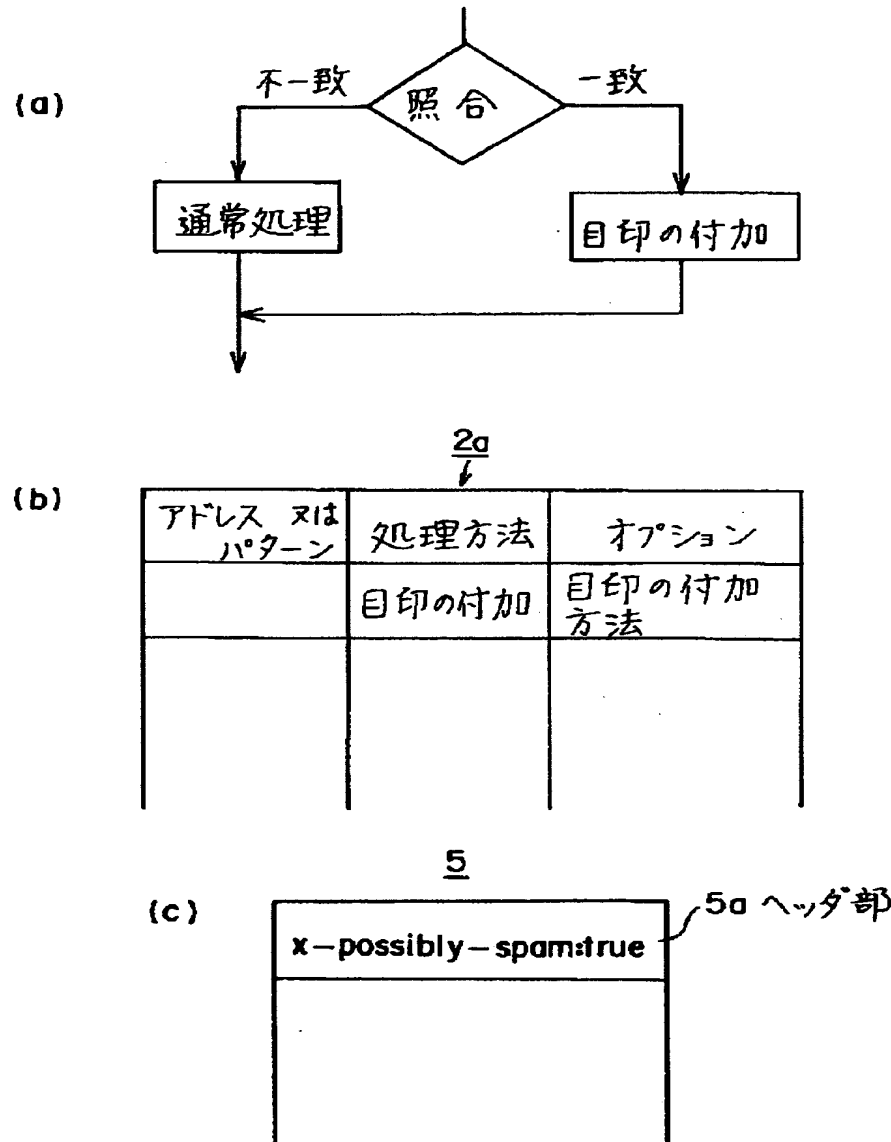
2a

アドレス又は パターン	処理方法	オプション
	エラーメール送出	なし

(b)

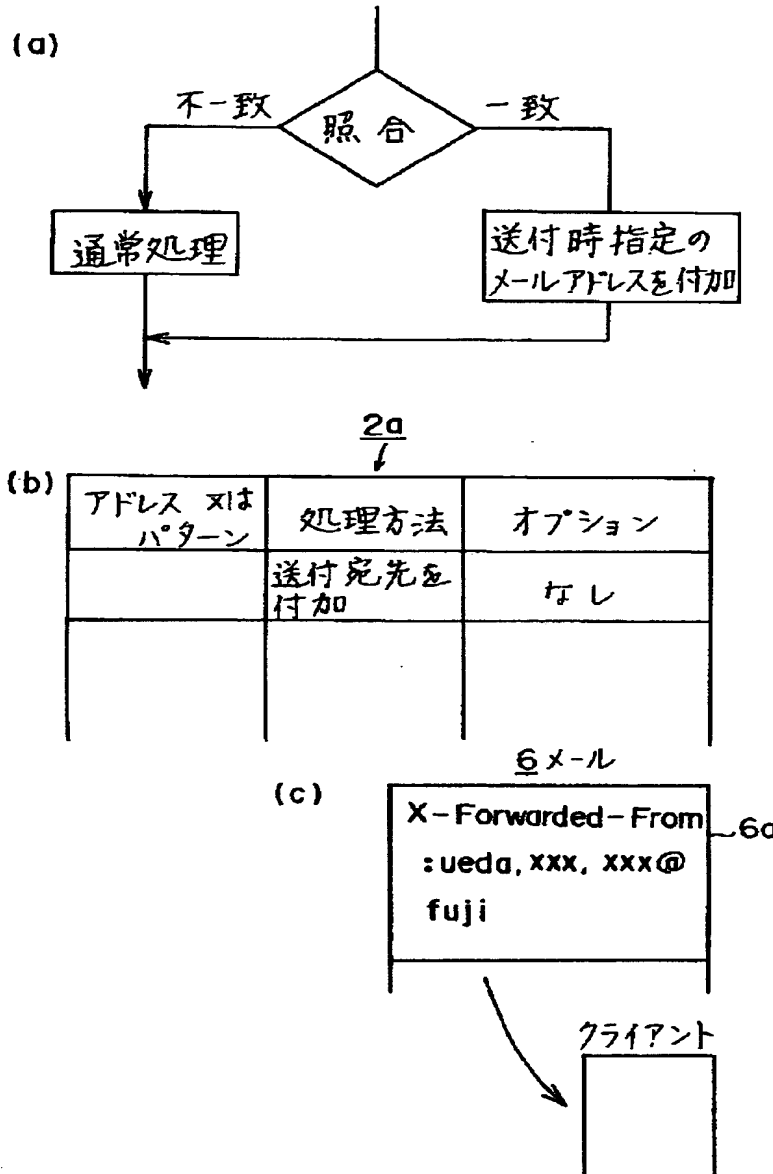
【図4】

サーバが通常のようにメールは配送するが、メッセージ中に指定された目印を加える処理を行う場合のメール受け付け部の処理、処理方法記憶部のテーブル及び目印の例を示した図



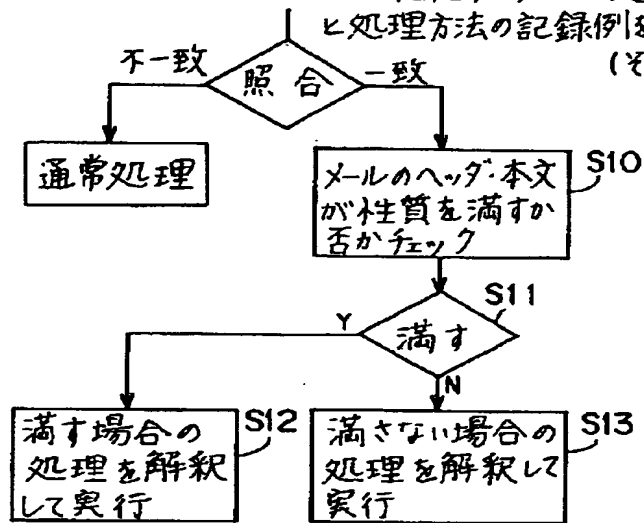
【図 5】

サーバが通常のようにメールは配送するが、届いたメールアドレスをメッセージ中に加える場合の処理内容、テーブル、処理例を示した図



【図 6】

届いたメールが特定の性質を持ったものかどうか
判定し、それによってメールの処理方法を指定するサーバの処理
と処理方法の記録例を示す図
(その1)



(a)

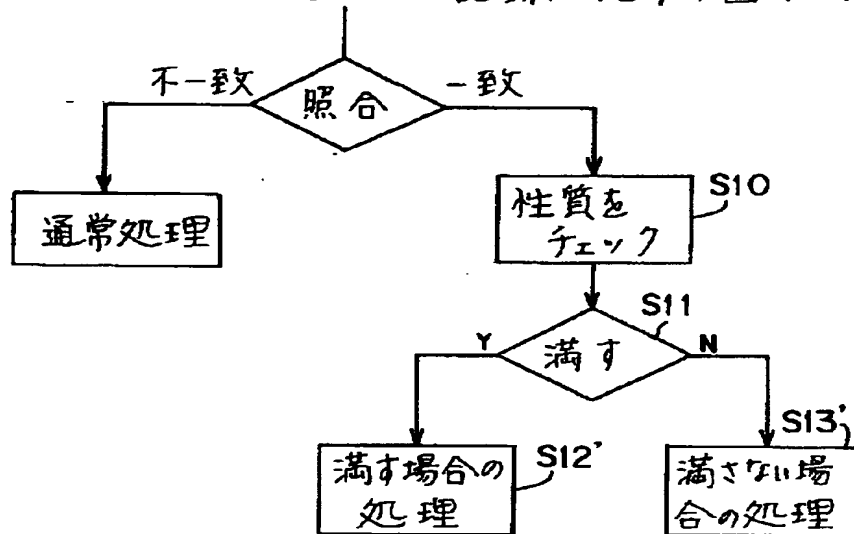
2a

アドレス 又はパターン	処理 方法	オプ ショ ン		
		性質の 記述	満す場合の 処理とその ためのオプション	満さない場合の 処理とそのた めのオプション
	性質によ り処理を 変える			

(b)

【図7】

届いたメールが特定の性質を持ったものかどうか判定し、それによってメールの処理方法を指定するサーバの処理と処理方法の記録例を示す図(その2)



(a)

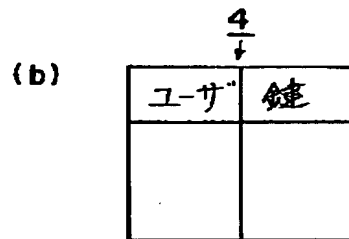
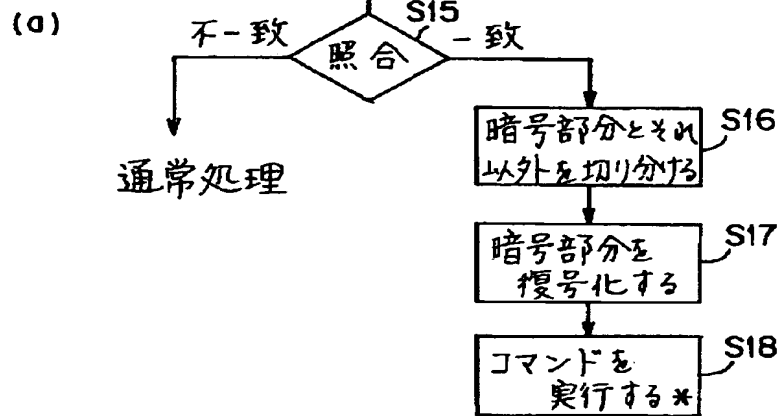
2a
↓

アドレス又は パターン	処理方法	オプション
	性質により 処理を変える	性質の記述

(b)

【図 8】

処理方法を暗号化してメールアドレスの任意文字列の中に埋め込んでおき、サーバはそれを解釈して実行する場合のサーバの処理と記憶されるデータを示す図(その1)



2a
↓

(c)

アドレス 又は パターン	処理方法	オプ ショ ン
	暗号化された コマンドを実行	暗号部分取出し パターン **

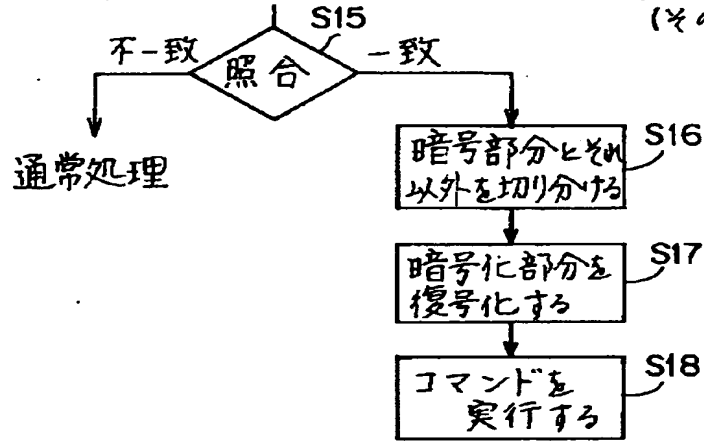
* 実行時に以下の情報のいずれかあるいは全てへの参照を可能にする。

- メール本体 (ヘッダ、本文)
- 取出しパターン
- メールアドレス

** 暗号切出しパターンはオプションでなくアドレスパターンの一部として指定保存しても良い。

【図 9】

処理方法を暗号化してメールアドレスの任意文字列の中に埋め込んでおき、サーバはそれを解釈して実行する場合のサーバの処理と記憶されるデータを示す図
(その2)



(a)

2a

アドレス 又はパターン	処理方法	オプション	
	暗号コマンド	暗号部分取出しパターン	鍵

(b)

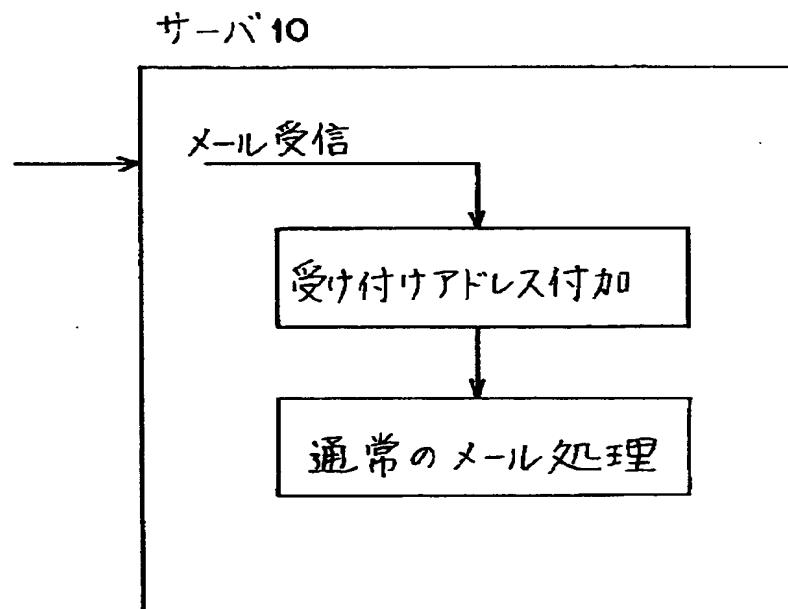
2a

アドレス 又はパターン	処理方法			オプション
	パターン(暗号部分取出し方法を含む)	暗号コマンド	鍵	

(c)

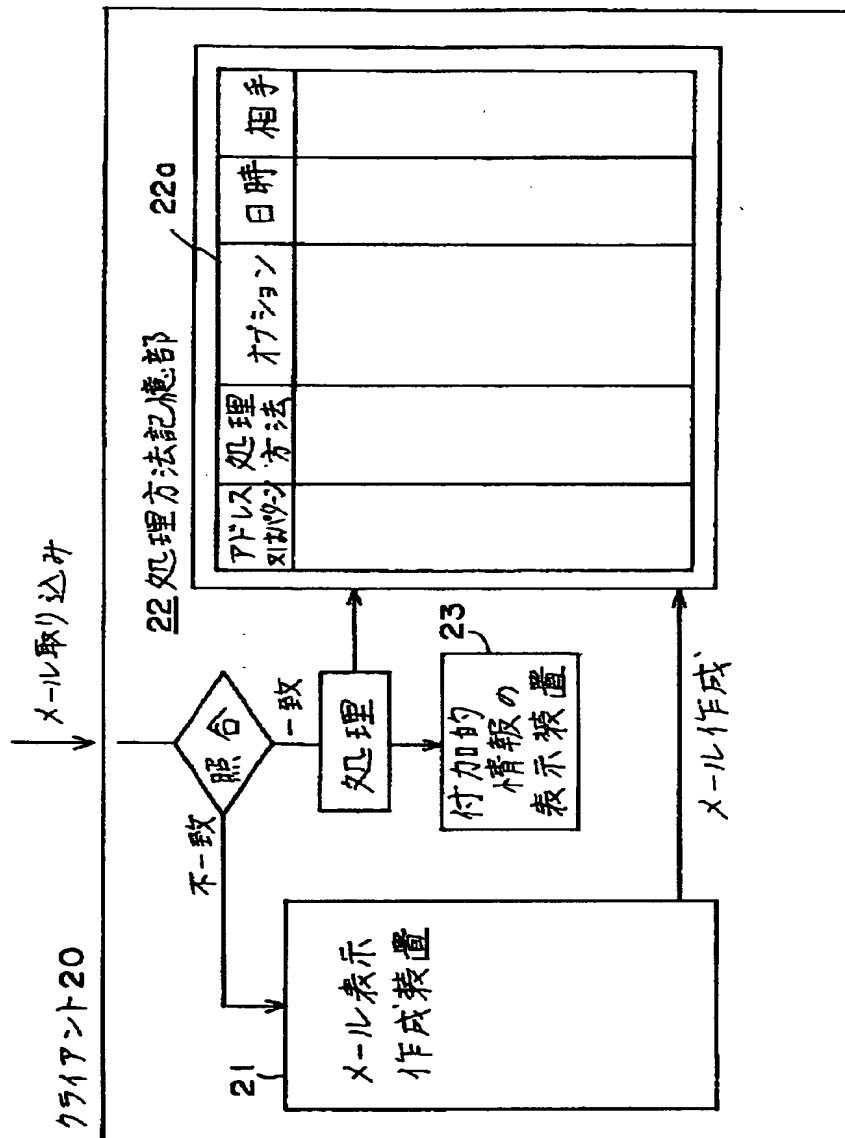
【図 10】

クライアントに悪戯メール防止装置を設ける
場合のサーバの処理を説明する図



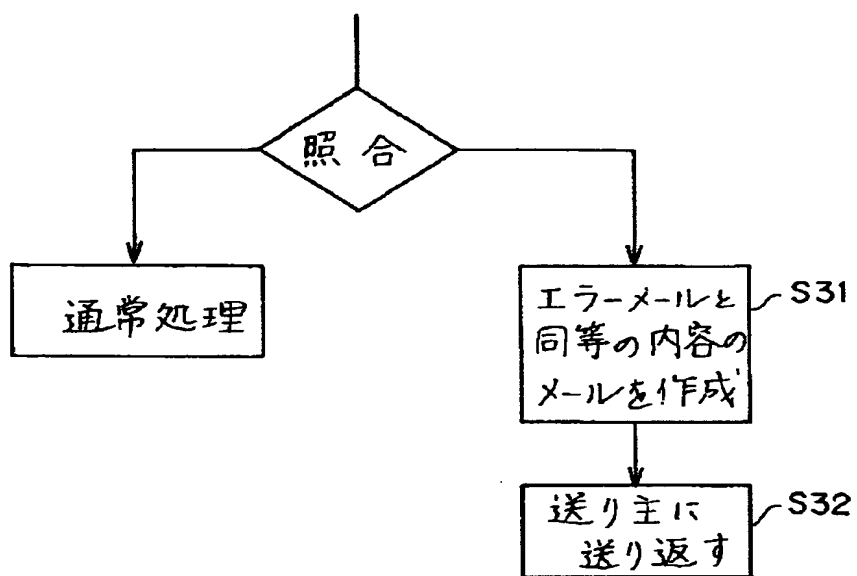
【図 1 1】

クライアントで悪戯メールの処理をする場合の
クライアントの構成を示す図



【図12】

エラーメールと同等の内容のメールを作成し、
これを送り主に送り返す場合の処理を示す図



【図 13】

クライアントのプログラムが、ユーザにフィールド名や日付を問い合わせるフォーマットの一例を示す図

30
↓

<p>受理 非受理</p> <div style="display: flex; justify-content: space-around;"> <div style="text-align: center;"> <input type="checkbox"/> 32 </div> <div style="text-align: center;"> <input checked="" type="checkbox"/> 31 </div> </div> <div style="display: flex; justify-content: space-around;"> <input type="checkbox"/> <input type="checkbox"/> </div>	<p>Subject <input type="text" value="パターン"/> 37</p> <p>to <input type="text" value="パターン"/> 38</p> <p>from <input type="text" value="パターン"/> 39</p>
<div style="display: flex; justify-content: space-between;"> <div>日付</div> <div style="text-align: right;"> from <input type="text"/> 35 to <input type="text"/> 36 </div> </div>	

【書類名】 要約書

【要約】

【課題】 悪戯メールの受信を防止することのできる装置及び方法を提供する。

【解決手段】 電子メールを配信するサーバ 1 は、各ユーザのための送信先として、ユーザが任意に決められる部分を持つ複数の送信先を受信する事ができ、伝送路からメールを受信すると、メール受け付け部 3 において、メールから送信アドレスを抽出し、それを処理内容記憶部 2 のテーブル 2 a に記憶されているアドレスあるいはアドレスパターンと照合する。一致しない場合には、そのユーザへの通常のメール処理を行い、一致する場合には、メールを破棄する、エラーメールを返送する、メールの所定領域に目印を添付する、送信先のアドレスを付加する、メールの有する性質に従った処理を行う。あるいは、アドレスに暗号化されたパターンが含まれている場合には、該パターンを復号して得られたコマンドに従った処理を行う。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [0 0 0 0 0 5 2 2 3]

1. 変更年月日 1 9 9 6 年 3 月 2 6 日

[変更理由] 住所変更

住 所 神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号

氏 名 富士通株式会社